AVA-79

Reference 1

PRIVACY COMMUNICATION SYSTEM

Publication number: JP5022283

Publication date: 1993-01-29

Inventor: TOTSUKA HISAYOSHI

Applicant: CATV KIBAN GIJUTSU KENKYUSHO

Classification:

- International: ***G09C1/00; H04K1/00; H04L9/06; H04L9/14;*** **G09C1/00; H04K1/00; H04L9/06; H04L9/14**; (IPC1-7): G09C1/00; H04K1/00; H04L9/06; H04L9/14

- european:

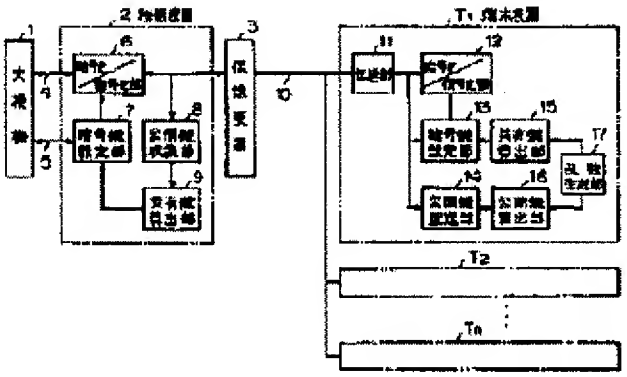
Application number: JP19910026402 19910220

Priority number(s): JP19910026402 19910220

Report a data error here

Abstract of **JP5022283**

PURPOSE:To revise a ciphering key for each call without need of key management and deterioration in the call connection quality. CONSTITUTION:Every time the collection of an open key in each of terminal equipments T1-Tn from a center is finished, a random number generating section 17 is started to generate a random number, an open public key is calculated from the random number and latched in an open public key delivery section 14, a common key is calculated, the common key is divided into plural ciphering keys and they are latched in a common key calculation section 15. The center collects the open public key from each terminal equipment periodically, calculates a common key corresponding to each terminal equipment and divides it to obtain plural ciphering keys. The center uses one by one ciphering key of a relevant terminal equipment sequentially for each call, informs the operating ciphering key to a relevant terminal equipment and ciphering/decoding is implemented by using a same ciphering key in the center terminal equipment to execute ciphering communication. Before the use of plural ciphering keys generated at once is not finished, a new open public key is generated to generate plural succeeding ciphering keys.



AVA-79

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－22283

(43)公開日　平成5年(1993)1月29日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		7922－5L			
Ｈ０４Ｋ	1/00	Ｚ	7117－5K			
			7117－5K	Ｈ０４Ｌ	9/02	Ｚ

審査請求　有　　請求項の数1(全　4　頁)

(21)出願番号　特願平3－26402

(22)出願日　平成3年(1991)2月20日

(71)出願人　591050039
株式会社シーエーテイブイ基盤技術研究所
東京都新宿区歌舞伎町1丁目2番3号

(72)発明者　戸塚　久義
東京都新宿区歌舞伎町1丁目2番3号　株式会社シーエーテイブイ基盤技術研究所内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　秘話通信方式

(57)【要約】

【目的】　鍵管理を不要とし、かつ呼接続品質を劣化することなく、呼毎に暗号鍵の変更を可能とする。

【構成】　各端末装置T_1～T_nではセンタから公開鍵の収集が終了するごとに乱数生成部１７を起動して乱数を生成し、その乱数から公開鍵を算出して公開鍵配送部１４に保持し、かつ共有鍵を算出し、その共有鍵を分割して複数の暗号鍵を作って共有鍵算出部１５に保持しておく。センタは周期的に各端末から公開鍵を収集し、各端末対応に共有鍵を演算し、更に分割して複数の暗号鍵を得る。センタは各呼ごとに対応端末の暗号鍵を１つずつ順に使用し、その使用暗号鍵を対応端末に通知し、センター端末内で同一暗号鍵で暗号化／復号化して秘密通信を行う。１回に生成した複数の暗号鍵を使用し終らないうちに、新らたな公開鍵を生成し、次の複数の暗号鍵を作っておく。

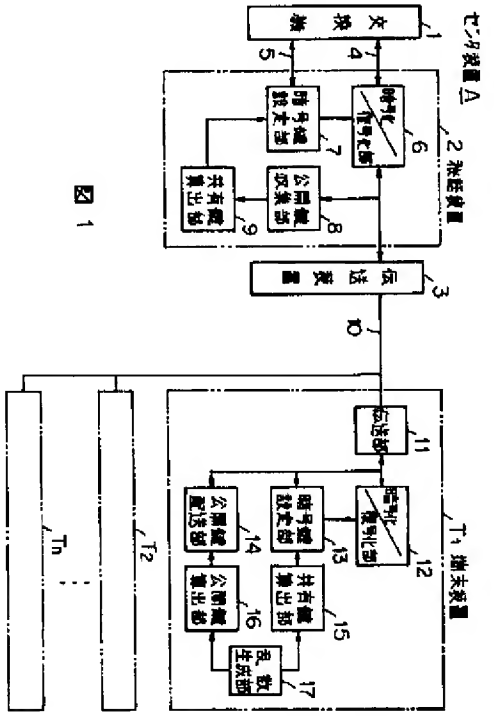


図１

1

【特許請求の範囲】

【請求項１】　センタ装置及び端末装置でそれぞれの秘密鍵から公開鍵を算出し、上記センタ装置と端末装置間でそれぞれの上記公開鍵を通信路にて授受し、お互いに自分の秘密鍵と相手の公開鍵とから、上記センタ装置と上記端末装置との間で共有の鍵を算出し、その共有の鍵を暗号鍵としてセンタ装置ー端末装置間での信号の暗号化／復号化を行って上記センタ装置を介して端末装置ー端末装置間で秘密通信を行う秘話通信方式において、

自分の秘密鍵と相手の公開鍵から算出した上記共有の鍵から複数の暗号鍵を取り出し、その複数の暗号鍵に番号を付与し、

その暗号鍵の番号を呼毎に通信路にて上記センタ装置から端末装置に対し、通知することにより、呼毎に使用する暗号鍵を変更し、

１つの上記共有の鍵から得られた複数の暗号鍵の全てを使い終わらない内に呼処理とは別のタイミングにて新たな公開鍵を算出して授受を行い、次段階の上記複数の暗号鍵を用意しておくことを特徴とした秘話通信方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明はセンタ装置及び端末装置でそれぞれの秘密鍵から公開鍵を算出し、その公開鍵をセンタ装置及び端末装置間で通信路を通じて授受し、お互いに自分の秘密鍵と相手の公開鍵とからセンタ装置と端末装置との間で共有の鍵を算出し、その共有の鍵を暗号鍵としてセンタ装置ー端末装置間での信号の暗号化／復号化を行って、センタ装置を介して端末装置ー端末装置間で秘密通信を行う秘話通信方式に関し、特に暗号鍵の配送に係わる。

【０００２】

【従来の技術】慣用暗号方式による暗号化は暗号鍵により行っており、鍵が異なれば復号できない。従来、この暗号鍵はそのものが製作時端末装置のＩＣ等に作り込まれるか、またはＩＣカード等の外部機器によってセットされていた。また、製作時に各端末装置全てに同じセンタ装置の公開鍵がセットされ、端末装置設置（電源投入）時に生成する疑似乱数によりセンタ装置に配送するための公開鍵及びセンタ装置の公開鍵から共有鍵が算出され、センタ装置も各端末装置からの公開鍵により各端末装置対応にその端末装置と共有な鍵が算出されることにより、暗号鍵がセットされていた。その他にも各端末装置固有のマスタ鍵が製作時ＩＣ等に作り込まれるか、またはＩＣカード等の外部機器によってセットされ、センタ装置あるいは各端末装置で生成した固有の値をマスタ鍵で暗号化し、そのデータを授受することにより暗号鍵を得ていた。

【０００３】

【発明が解決しようとする課題】このように従来の暗号鍵配送方式では、暗号鍵そのものまたはマスタ鍵を製作

2

時ＩＣ等に作り込むか、あるいはＩＣカード等の外部機器によってセットした場合には鍵の設定・変更において鍵管理が必要であったり、そのための製作費または工事費が必要であった。

【０００４】また、公開鍵配送方式では暗号鍵の生成に多くの計算量を要することから計算時間を多く必要とするため、呼接続毎に暗号鍵を変更しようとして呼接続毎に暗号鍵を計算させることは接続品質上好ましくなく、従って、従来では端末装置設置時にのみ公開鍵授受による暗号鍵の設定を行っていた。このため、高い安全性が得られなかった。

【０００５】この発明の目的はこのような課題を解決するためになされたもので、オペレータが暗号鍵を意識しないでシステムの運用ができ、製造業者、工事業者も暗号鍵を意識しないで製造・工事ができ、しかも呼接続毎に呼接続許容時間以内に暗号鍵を替えることができ、暗号化強度をより高め、つまり安全性の高い秘密通信方式を提供することにある。

【０００６】

【課題を解決するための手段】この発明によれば秘密鍵と相手の公開鍵とから演算した共有の鍵から複数の暗号鍵を取り出し、その各暗号鍵に番号を付与し、呼毎に使用する暗号鍵の番号をセンタ装置から端末装置へ通知し、呼毎に使用する暗号鍵を変更する。一方、１つの共有の鍵から得られた複数の暗号鍵を全て使用し終わらない内に、呼処理とは別のタイミングで新たな公開鍵を算出してセンタ装置ー端末装置間でその公開鍵の授受を行い、次段階に用いる複数の暗号鍵を用意しておく。

【０００７】

【作用】この発明によれば、公開鍵方式を用い暗号鍵に関して、端末装置製造時または設置時に固有の値をセットする必要がなく、鍵管理も必要がない。また、予め暗号鍵を演算しておくから、呼接続許容時間以内に暗号鍵の設定ができることから良好な接続品質で電話システムに対する秘話が可能となり且つ、呼接続毎に暗号鍵の変更をすることから盗聴に対する強度が大きい。

【０００８】

【実施例】以下、図１を参照して、この発明の一実施例を説明する。この実施例は時分割多重通信方式にこの発明を適用した場合である。センタ装置Ａは交換機１、秘話装置２及び伝送装置３から構成され、秘話装置２は暗号化／復号化部６、暗号鍵設定部７、公開鍵収集部８及び共有鍵算出部９から成る。端末装置T_1 ～T_n はそれぞれ伝送部１１、暗号化／復号化部１２、暗号鍵設定部１３、公開鍵配送部１４、共有鍵算出部１５、公開鍵算出部１６及び乱数生成部１７から成る。

【０００９】センタ装置Ａから各端末装置T_1 ～T_n への放送用、公開鍵収集用及び通話用等の下り情報は時分割され、伝送装置３にて搬送波を変調して、伝送路１０を通じて各端末装置T_1 ～T_n に全て伝送される。端末

装置T_1～T_nからの公開鍵配送用及び通話用等の上り情報も各端末装置において時分割されたそれぞれのタイムスロットにセットされ、伝送部１１により下りの搬送波周波数とは別搬送波周波数を変調して伝送路１０を通じてセンタ装置Ａに伝送される。

【００１０】交換機１は送信しようとする端末装置に対し、放送用タイムスロットにより通話のためのタイムスロットを指示し、このタイムスロットに通話データをのせて端末装置T_1～T_nに送り出す。当該端末装置はこのタイムスロットを取り出してセンタ装置Ａからの通話データを受け取る。当該端末装置においても交換機１から指示された上り用タイムスロットに通話データをのせてセンタ装置Ａに送り出す。このとき交換機１からの下り通話データに対し、秘話装置２は交換機１から制御データ授受信号路５を通して指示されたタイムスロットの通話データを該当する端末装置の暗号鍵で暗号化する。当該端末装置はこの通話データを受け取り、同じ暗号鍵で復号する。当該端末装置は上り通話データも同じ暗号鍵で暗号化し、センタ装置Ａに伝送する。センタ装置Ａでは秘話装置２によりそのタイムスロットの通話データを同じ暗号鍵で復号し、交換機１に送る。このようにしてセンタ装置と端末装置との通話データに対して暗号化／復号化を行い、秘密通話を行う。

【００１１】公開鍵収集と共有鍵算出は上記の通話とは非同期で行う。公開鍵収集は収集するためのタイムスロットを予め割り当てておき、秘話装置２からのポーリングにより各端末装置T_1～T_nに対して一定時間毎に行う。この一定時間とは１つの公開鍵から得られた複数の暗号鍵の数と呼率により決定する。つまりその一定時間内に発生した各呼ごとに異なる暗号鍵を割当てた時に暗号鍵が不足しないように上記一定時間を設定する。秘話装置２が公開鍵収集用タイムスロットを通じて指定した端末装置T_iに対し、配送要求を出すと、その端末装置T_iの公開鍵配送部１４は既に公開鍵算出部１６にて算出されている公開鍵を上りの配送用タイムスロットにて送出する。センタ装置Ａはその端末装置T_iの公開鍵を公開鍵収集部８にて収集すると、その公開鍵と自己の秘密鍵とから共有鍵算出部９にてその端末装置T_iとの共有鍵を算出し、この共有鍵を例えばビット分割して複数の暗号鍵を得る。これらの暗号鍵に対し予め決めた順番に番号を付与し、更に現在使われている暗号鍵と区別するために属性データも付与する。属性データはセンタ装置Ａ、端末装置共、初期値を「０」とし、以降「１」と「０」を繰り返す。

【００１２】端末装置T_1～T_nにおいては電源投入時（初期時）及びセンタ装置Ａに対して公開鍵を配送した時に乱数生成部１７により乱数を生成し、この乱数値から公開鍵算出部１６により例えば一方向性関数を使って公開鍵が算出される。この乱数は各端末装置T_1～T_nに設定されるＩＤ（識別）番号等との組み合せにより端末装置毎に固有の値となるようにする。更に、この乱数値と予め設定されているセンタ装置Ａの公開鍵とにより共有鍵算出部１５は共有鍵を算出する。この時、秘話装置２と同様な方法でこの共有鍵を例えばビット分割して複数の暗号鍵を得、これらの暗号鍵に対しその決めた順番に番号を付与すると共に、属性を与える。このようにして公開鍵算出部１６に得られた公開鍵は、次に秘話装置２から収集要求がある迄保持しており、共有鍵算出部１５に得られた暗号鍵は公開鍵送出後、秘話装置２からの暗号鍵指示においてその属性が切り替えられていると、これにより使用されることになる。センタ装置からの公開鍵収集要求に対して送出を完了後、各端末装置は次の公開鍵および共有鍵を生成する処理を起動する。

【００１３】交換機１は端末装置T_1～T_nとの通信に先立ち、暗号鍵の設定を行うために、秘話装置２に対して端末名と使用タイムスロット指示及び暗号鍵番号の問い合わせを制御データ授受信号路５を通じて行う。秘話装置２の暗号鍵設定部７は指示のあった端末装置T_iの暗号鍵属性と暗号鍵番号とを交換機１に応答する。その暗号鍵番号は呼ごとに順次変更する。交換機１ではこの暗号鍵属性と番号を放送用タイムスロットを使ってその端末装置T_iに通知する。端末装置T_iは通知された属性及び番号の暗号鍵を暗号鍵設定部１３に設定し、また秘話装置２もその属性及び番号の暗号鍵を暗号鍵設定部７に設定する。

【００１４】暗号鍵設定が行われた後、秘話装置２の暗号鍵設定部７は暗号化／復号化部６に対し交換機１から指示されたタイムスロット及び暗号鍵を指示する。暗号化／復号化部６はデータ通信部４によって送られてきた交換機１からの下りデータのそのタイムスロットのデータを当該端末装置T_iの暗号鍵で暗号化する。また、伝送装置３からの上りデータのそのタイムスロットのデータもその端末装置T_iの暗号鍵で復号化する。端末装置T_iにおいても暗号化／復号化部１２では暗号鍵設定部１３からのタイムスロット番号及び暗号鍵の指示により下りデータの復号化、上りデータの暗号化を行う。このようにして交換機１と端末装置T_iとの通信データに対して暗号化／復号化を行い、データ授受を行う。

【００１５】センタ装置では公開鍵の収集を行い、共有鍵を演算し、複数の暗号鍵を得ると、次からその新たな暗号鍵を使用する。この時、それまで用いた暗号鍵と、新たな暗号鍵とは属性データにより区別される。

【００１６】

【発明の効果】以上説明したようにこの発明によれば鍵管理が不要になり、呼処理とは別のタイミングで新たな公開鍵、共有鍵と複数の暗号鍵との生成を行って予め準備してあるから、通話毎に暗号鍵の変更を、呼接続許容時間以内に可能となり、呼接続品質を劣化することがなく、かつ通話毎に暗号鍵を変更するため高い秘密性が得られる。

5

【図面の簡単な説明】

6

【図１】この発明の一実施例を示すブロック図。

【図１】

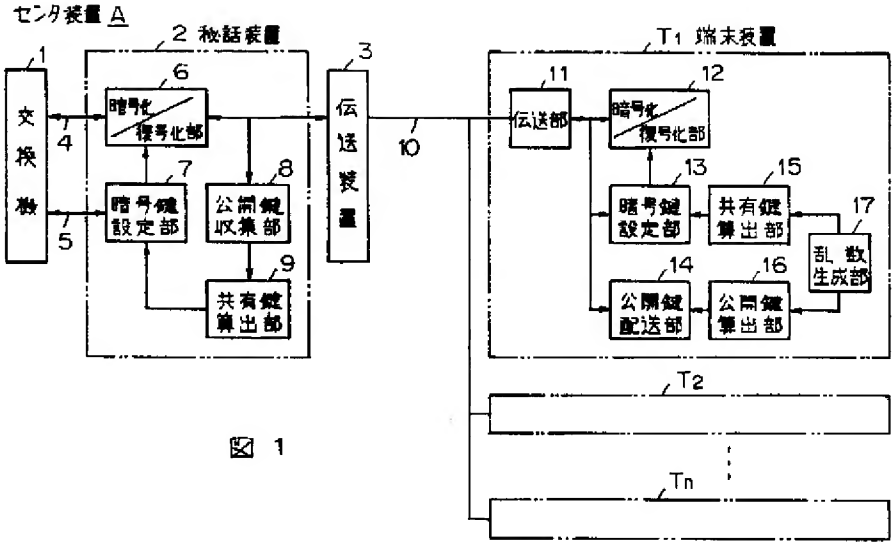


図 1